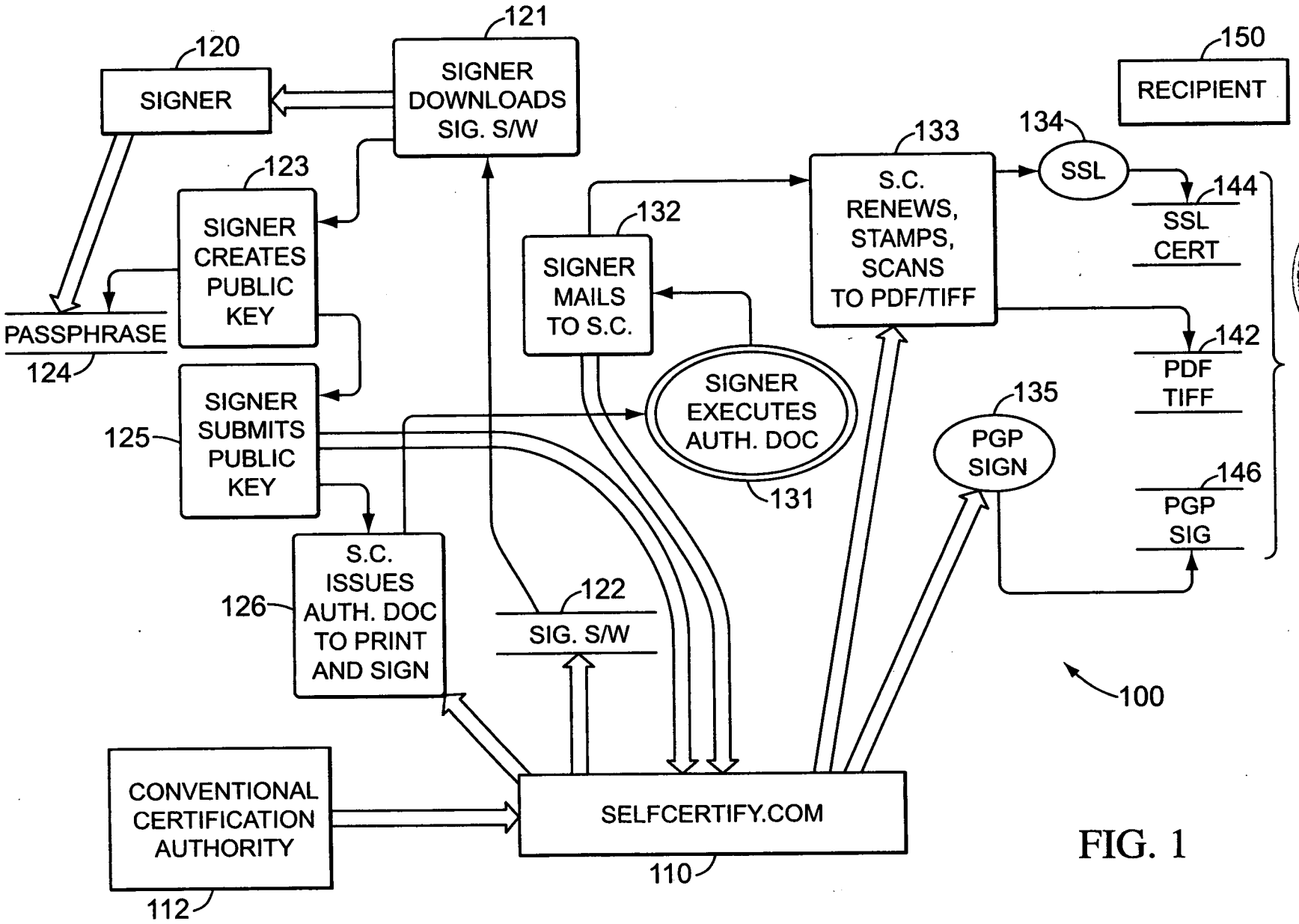


FIG. 1

NEW SHEET

1/18

S/N 10/093,943

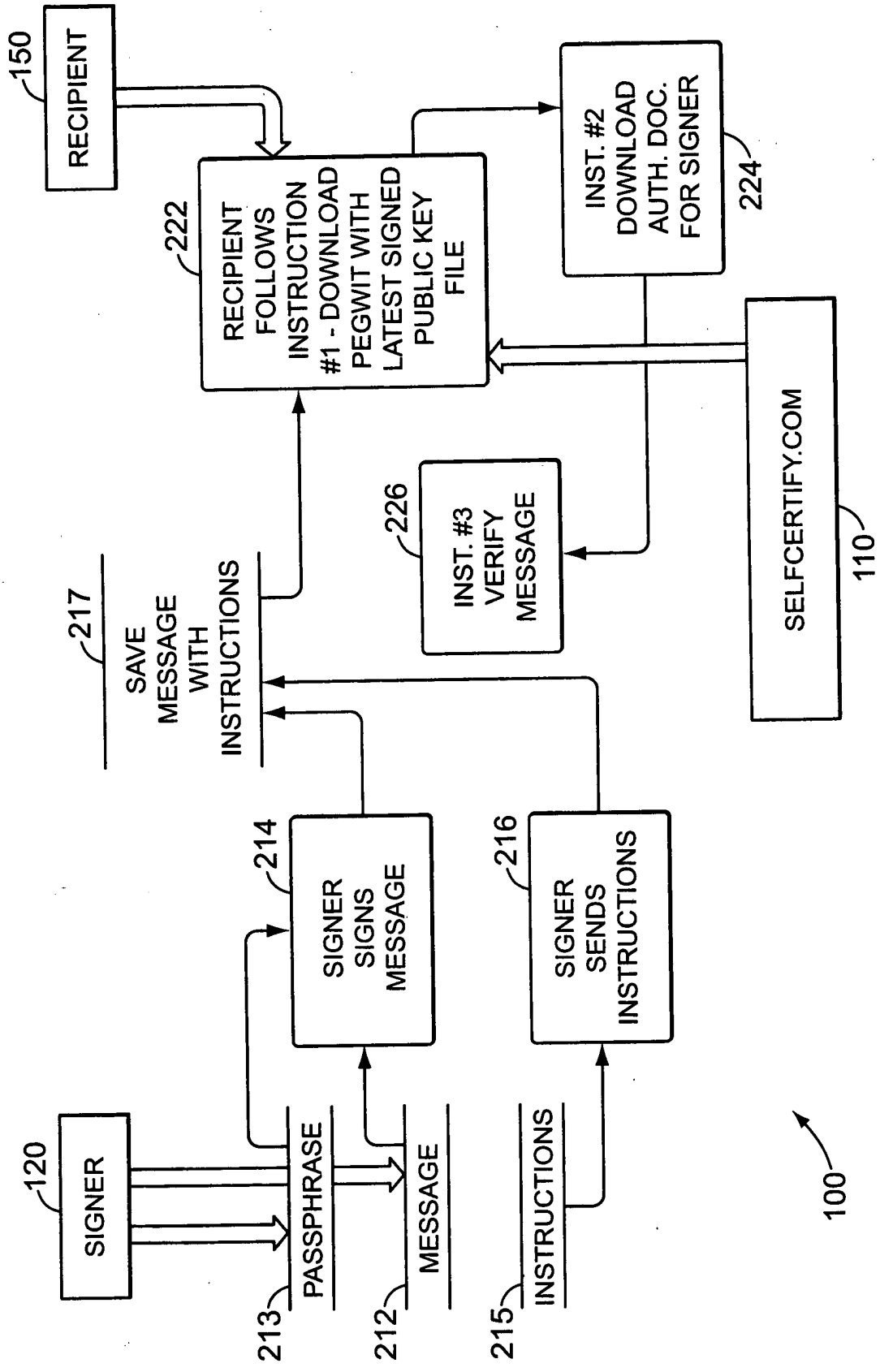

150
RECIPIENT
222
RECIPIENT FOLLOWS INSTRUCTION #1 - DOWNLOAD PEGWIT WITH LATEST SIGNED PUBLIC KEY FILE
224
INST. #2 DOWNLOAD AUTH. DOC. FOR SIGNER
226
INST. #3 VERIFY MESSAGE
110
SELFCERTIFY.COM
217
SAVE MESSAGE WITH INSTRUCTIONS
214
SIGNER SIGNS MESSAGE
216
SIGNER SENDS INSTRUCTIONS
120
SIGNER
213
PASSPHRASE
212
MESSAGE
215
INSTRUCTIONS
100

FIG. 2

FIG. 3

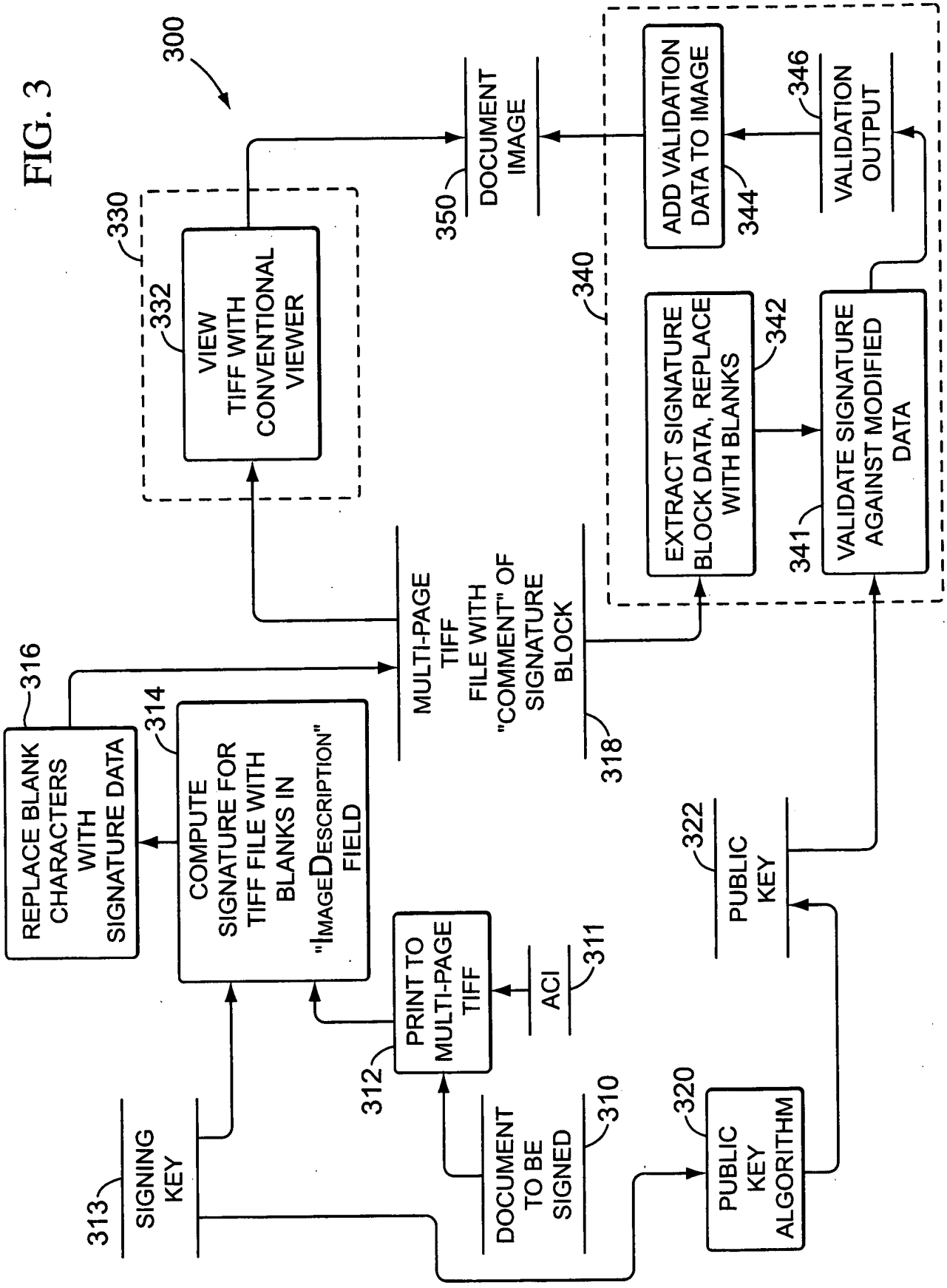
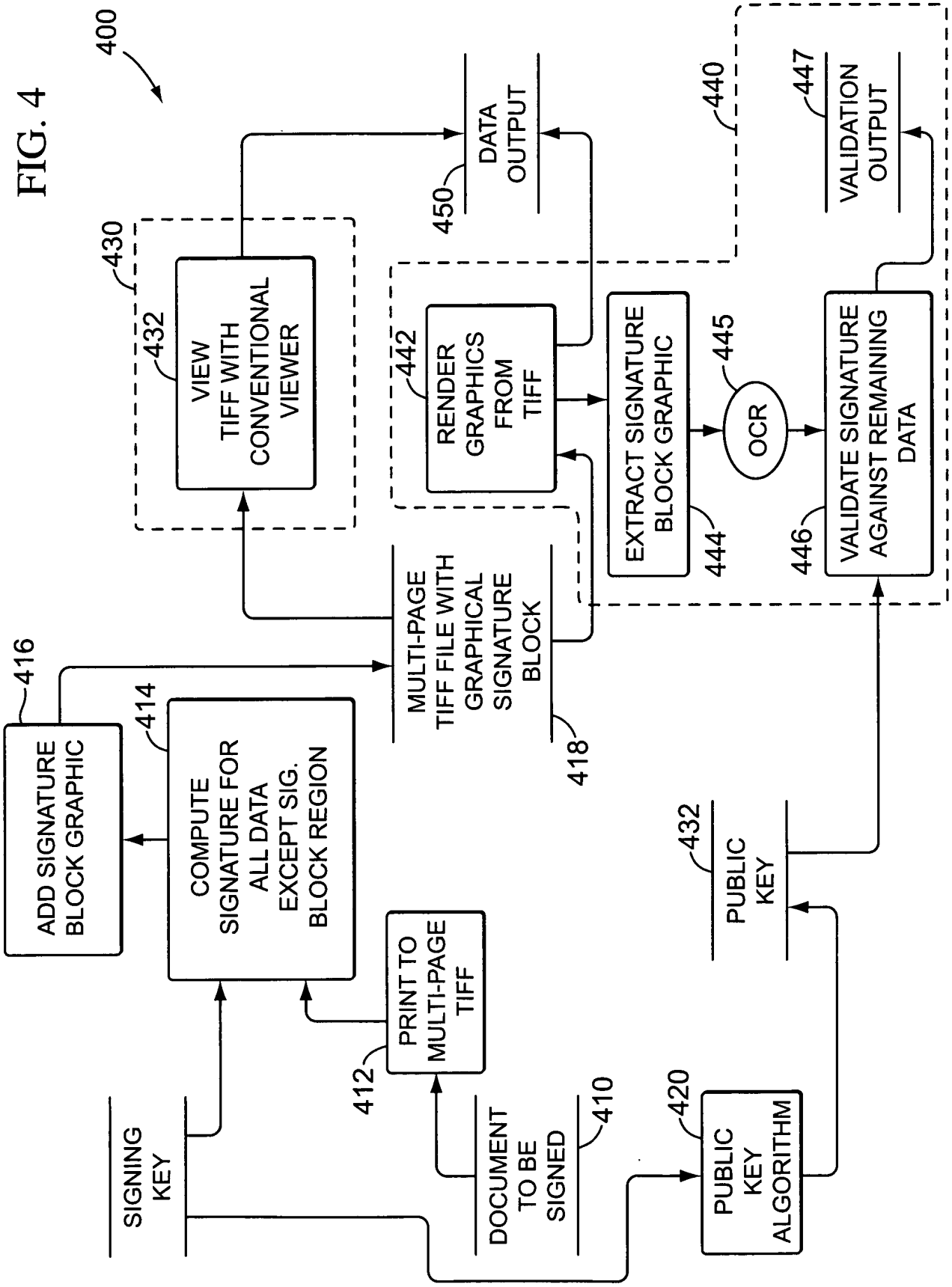
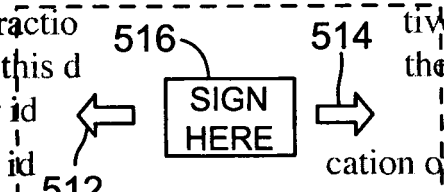

300
330
332
VIEW TIFF WITH CONVENTIONAL VIEWER
350
DOCUMENT IMAGE
340
ADD VALIDATION DATA TO IMAGE
344
346
VALIDATION OUTPUT
EXTRACT SIGNATURE BLOCK DATA, REPLACE WITH BLANKS
342
VALIDATE SIGNATURE AGAINST MODIFIED DATA
341
316
REPLACE BLANK CHARACTERS WITH SIGNATURE DATA
314
COMPUTE SIGNATURE FOR TIFF FILE WITH BLANKS IN "IMAGEDESCRIPTION" FIELD
MULTI-PAGE TIFF FILE WITH "COMMENT" OF SIGNATURE BLOCK
318
322
PUBLIC KEY
PRINT TO MULTI-PAGE TIFF
ACI
311
312
313
SIGNING KEY
DOCUMENT TO BE SIGNED
310
320
PUBLIC KEY ALGORITHM

FIG. 4


400
SIGNING KEY
DOCUMENT TO BE SIGNED
410
PRINT TO MULTI-PAGE TIFF
412
COMPUTE SIGNATURE FOR ALL DATA EXCEPT SIG. BLOCK REGION
414
ADD SIGNATURE BLOCK GRAPHIC
416
MULTI-PAGE TIFF FILE WITH GRAPHICAL SIGNATURE BLOCK
418
PUBLIC KEY ALGORITHM
420
PUBLIC KEY
432
VIEW TIFF WITH CONVENTIONAL VIEWER
430
RENDER GRAPHICS FROM TIFF
442
EXTRACT SIGNATURE BLOCK GRAPHIC
444
OCR
445
VALIDATE SIGNATURE AGAINST REMAINING DATA
446
440
DATA OUTPUT
450
VALIDATION OUTPUT
447

To verify a digital signature, the viewer searches the graphical rendering of the signed document for the distinctive graphical outline of the signature block. Distinctive features of the graphical outline can include (1) a distinctive color such as maroon, (2) a distinctive line shape such as double parallel lines, and (3) a distinctive line weight such as 3.2 points (not an integer or x.5 fractio tive properties are present in the simulated signature block for this d the signature block can have a predetermined size to further id



Once the viewer software has id cation of the signature block, it removes all of the graphic data of t ature block (up to and including the border) and sets it to the default blank value used during signature calculation. It performs an optical character recognition of the signature data within the block to obtain the value of the digital signature. According to advantageous aspects of the invention disclosed elsewhere, the digital signature can be applied to a secure delay to obtain another, larger digital signature value. The digital signature value (as shown or as expanded through a secure delay) is then validated against the modified TIFF representation of the document.

Very truly yours,

500

Edwin A. Suominen

FIG. 5

To verify a digital signature, the viewer searches the graphical rendering of the signed document for the distinctive graphical outline of the signature block. Distinctive features of the graphical outline can include (1) a distinctive color such as maroon, (2) a distinctive line shape such as double parallel lines, and (3) a distinctive line weight such as 3.2 points (not an integer or x.5 fraction). All of these distinctive properties are present in the simulated signature block for this document. In addition, the signature block can have a predetermined size to further identify it.

Once the viewer software has identified the exact location of the signature block, it removes all of the graphic data of the signature block (up to and including the border) and sets it to the default blank value used during signature calculation. It performs an optical character recognition of the signature data within the block to obtain the value of the digital signature. According to advantageous aspects of the invention disclosed elsewhere, the digital signature can be applied to a secure delay to obtain another, larger digital signature value. The digital signature value (as shown or as expanded through a secure delay) is then validated against the modified TIFF representation of the document.

500

Very truly yours,

600

-SelfCertify.com Digital Signature-
1410-2708-9007-5781-6673
7701-3376-8745-3789-9100
7440-2788-7101-4089-2409
5420-2178-9001-7680-1477
7731-3376-2645-3789-9105

Edwin A. Suominen

FIG. 6

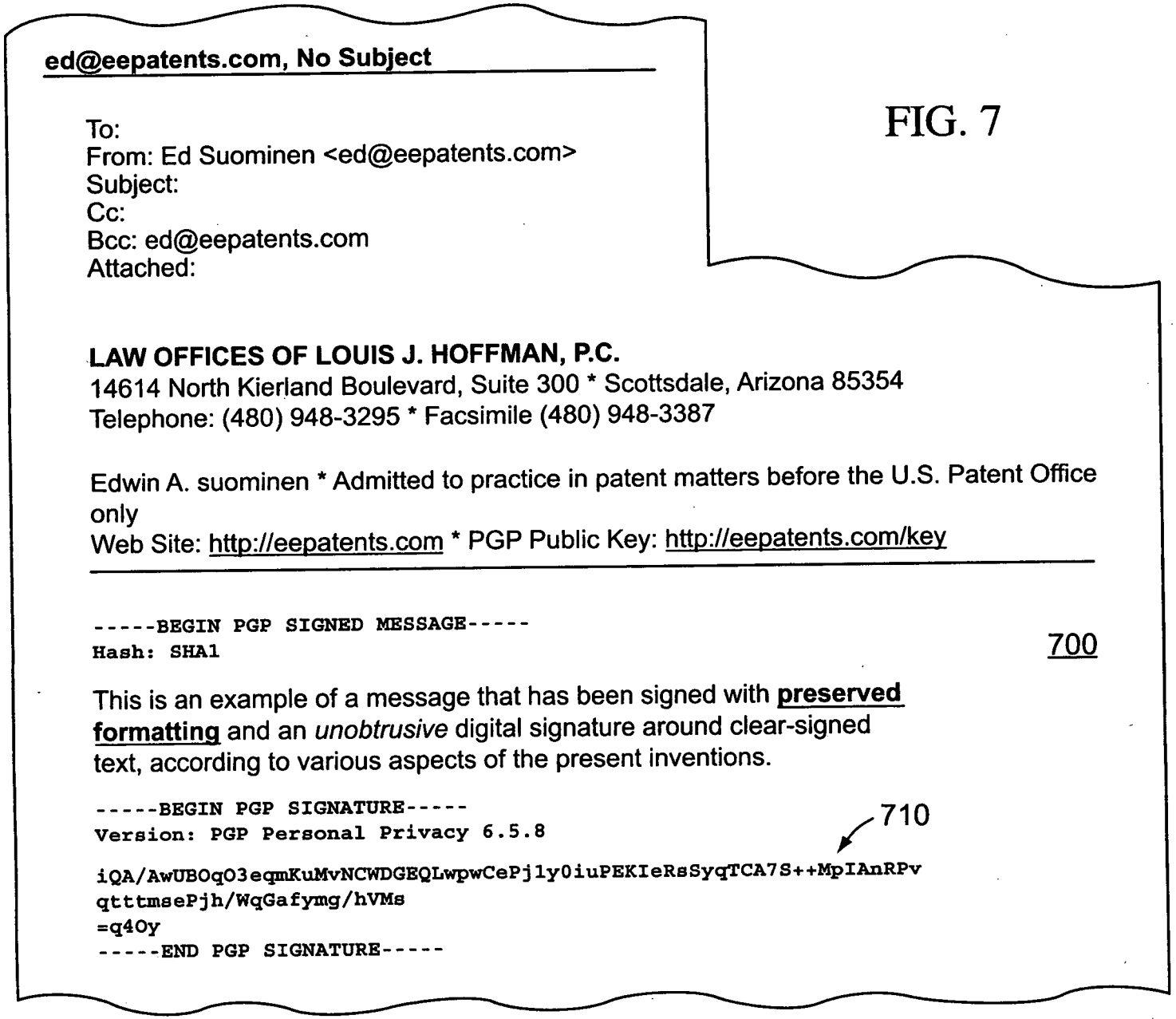

ed@eepatents.com, No Subject
To:
From: Ed Suominen <ed@eepatents.com>
Subject:
Cc:
Bcc: ed@eepatents.com
Attached:
LAW OFFICES OF LOUIS J. HOFFMAN, P.C.
14614 North Kierland Boulevard, Suite 300 * Scottsdale, Arizona 85354
Telephone: (480) 948-3295 * Facsimile (480) 948-3387
Edwin A. suominen * Admitted to practice in patent matters before the U.S. Patent Office only
Web Site: http://eepatents.com * PGP Public Key: http://eepatents.com/key
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
700
This is an example of a message that has been signed with preserved formatting and an unobtrusive digital signature around clear-signed text, according to various aspects of the present inventions.
-----BEGIN PGP SIGNATURE-----
Version: PGP Personal Privacy 6.5.8
710
iQA/AwUBOqO3eqmKuMvNCWDGEQLwpwCePj1y0iuPEKIeRsSyqTCA7S++MpIAnRPv
qtttmsePjh/WqGafymg/hVMs
=q4Oy
-----END PGP SIGNATURE-----

FIG. 7

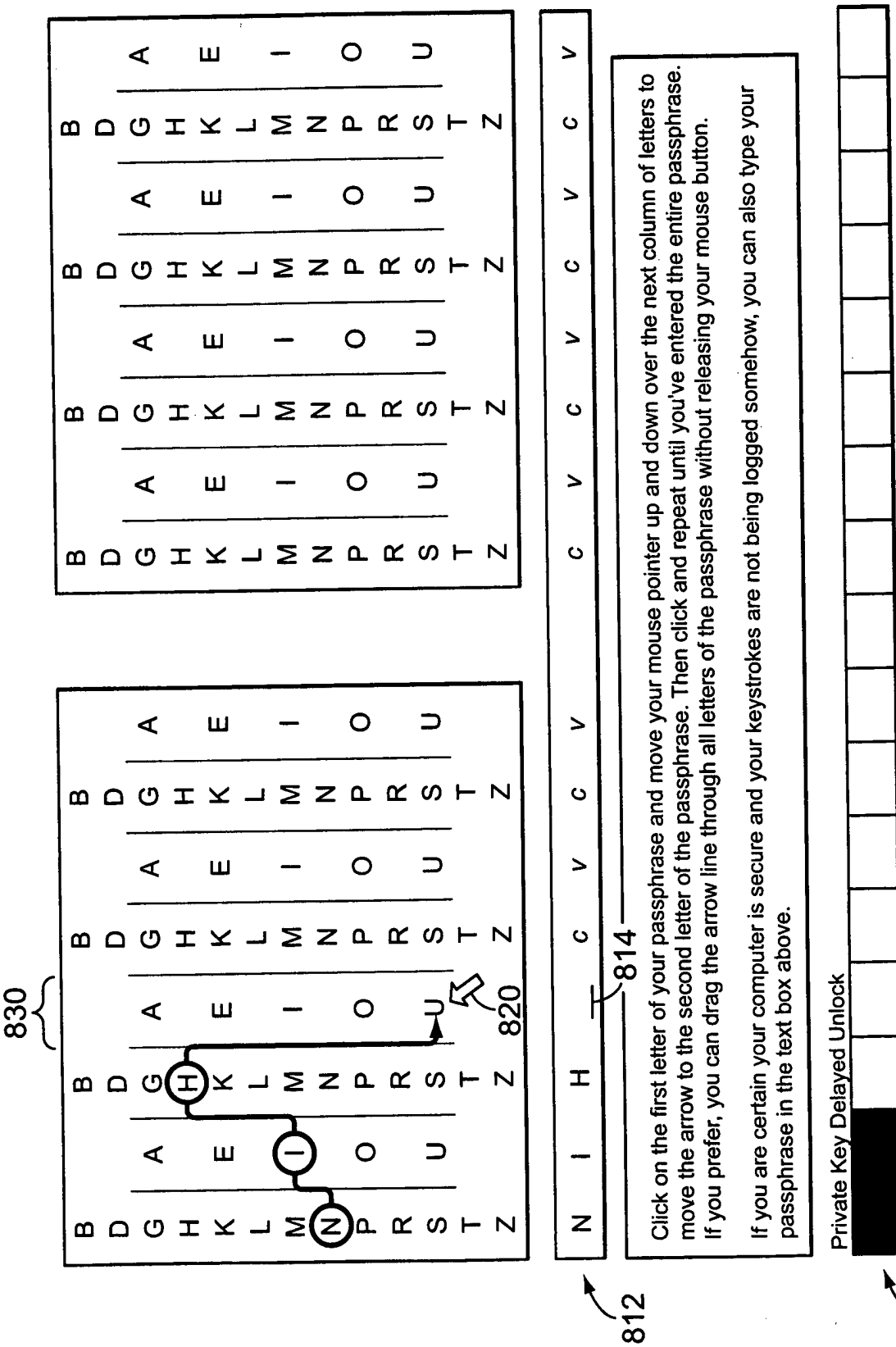

830
820
814
812
840
Click on the first letter of your passphrase and move your mouse pointer up and down over the next column of letters to move the arrow to the second letter of the passphrase. Then click and repeat until you've entered the entire passphrase. If you prefer, you can drag the arrow line through all letters of the passphrase without releasing your mouse button.
If you are certain your computer is secure and your keystrokes are not being logged somehow, you can also type your passphrase in the text box above.
Private Key Delayed Unlock

FIG. 8

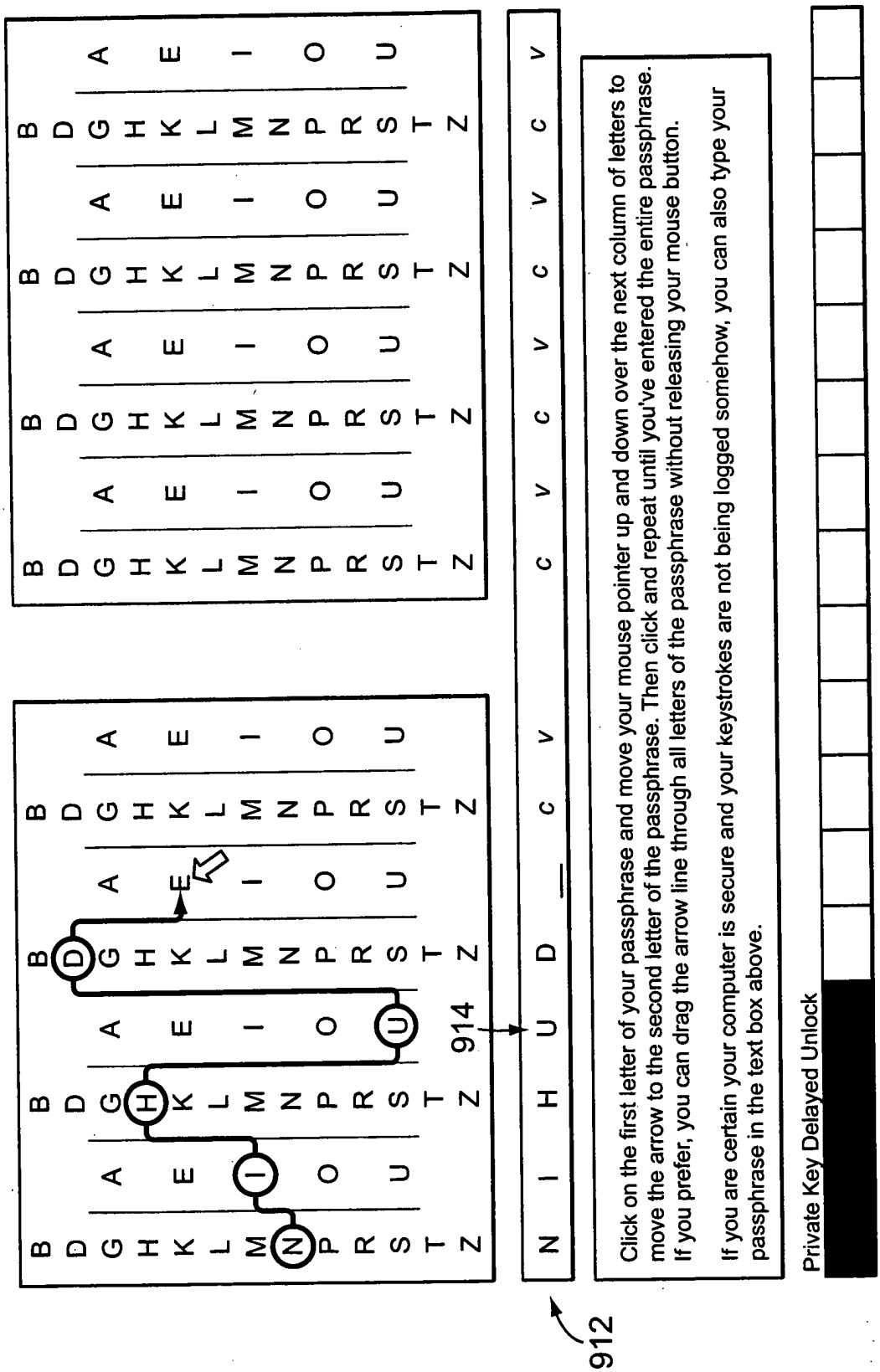

B D G H K L M N P R S T Z
A E I O U
N I H U D
c v c v c v c v
912
914
Click on the first letter of your passphrase and move your mouse pointer up and down over the next column of letters to move the arrow to the second letter of the passphrase. Then click and repeat until you've entered the entire passphrase. If you prefer, you can drag the arrow line through all letters of the passphrase without releasing your mouse button.
If you are certain your computer is secure and your keystrokes are not being logged somehow, you can also type your passphrase in the text box above.
Private Key Delayed Unlock
840

FIG. 9

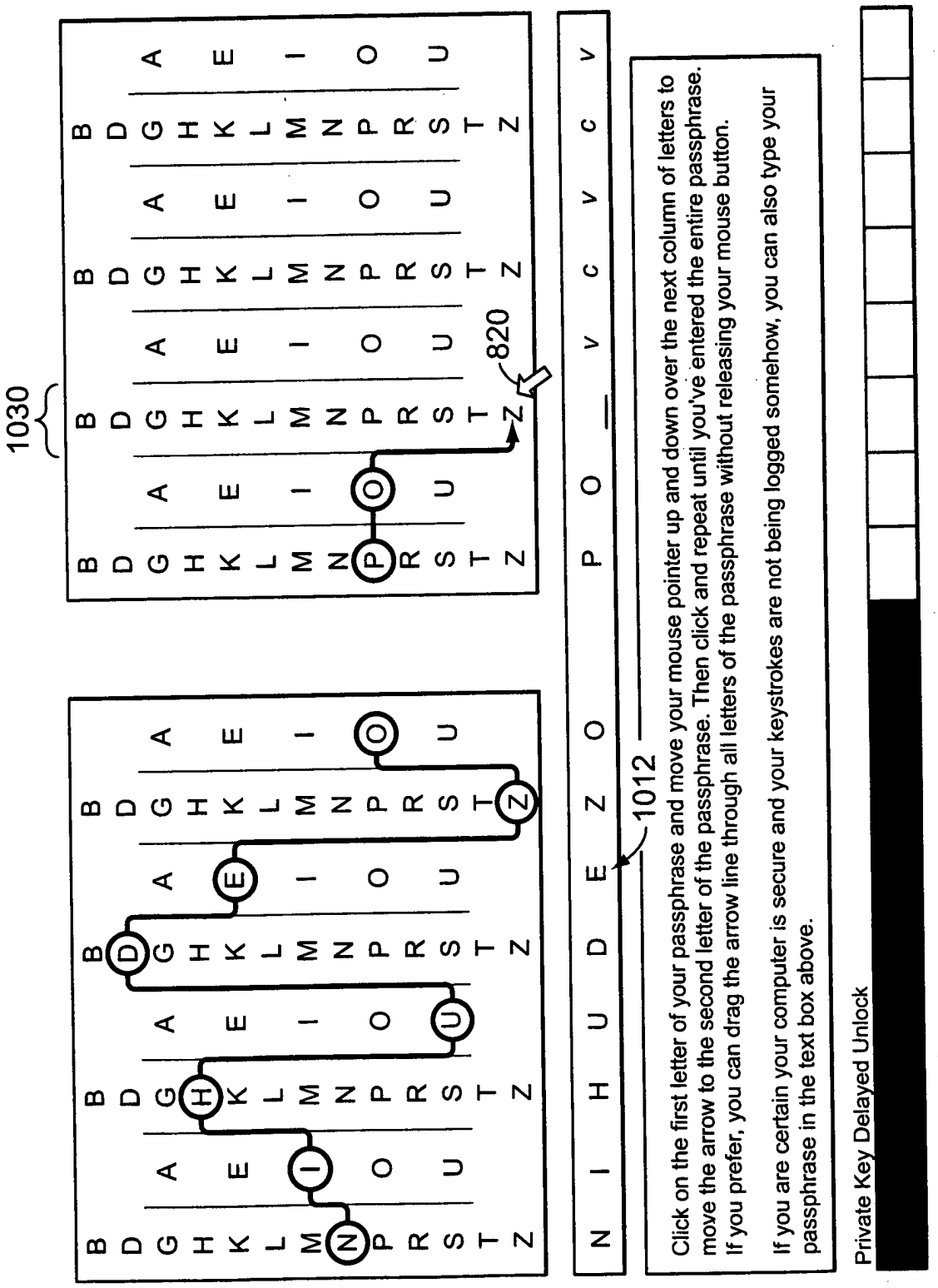

1030
820
1012
840
Click on the first letter of your passphrase and move your mouse pointer up and down over the next column of letters to move the arrow to the second letter of the passphrase. Then click and repeat until you've entered the entire passphrase. If you prefer, you can drag the arrow line through all letters of the passphrase without releasing your mouse button.
If you are certain your computer is secure and your keystrokes are not being logged somehow, you can also type your passphrase in the text box above.
Private Key Delayed Unlock

FIG. 10

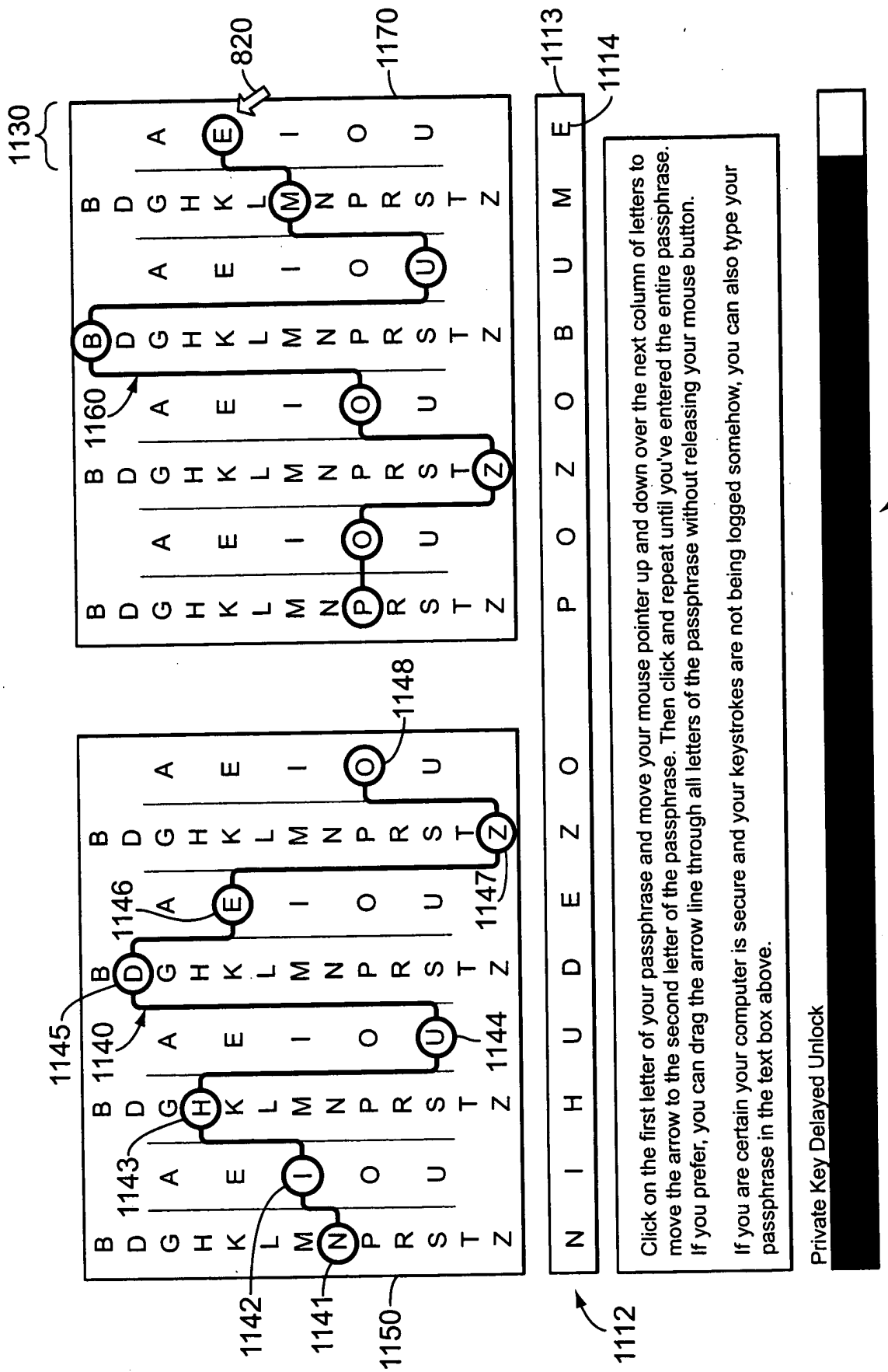

1130
820
1170
1160
1113
1114
1148
1145
1140
1146
1147
1144
1143
1142
1141
1150
1112
840
N I H U D E Z O P O Z O B U M E
Click on the first letter of your passphrase and move your mouse pointer up and down over the next column of letters to move the arrow to the second letter of the passphrase. Then click and repeat until you've entered the entire passphrase. If you prefer, you can drag the arrow line through all letters of the passphrase without releasing your mouse button.
If you are certain your computer is secure and your keystrokes are not being logged somehow, you can also type your passphrase in the text box above.
Private Key Delayed Unlock

FIG. 11

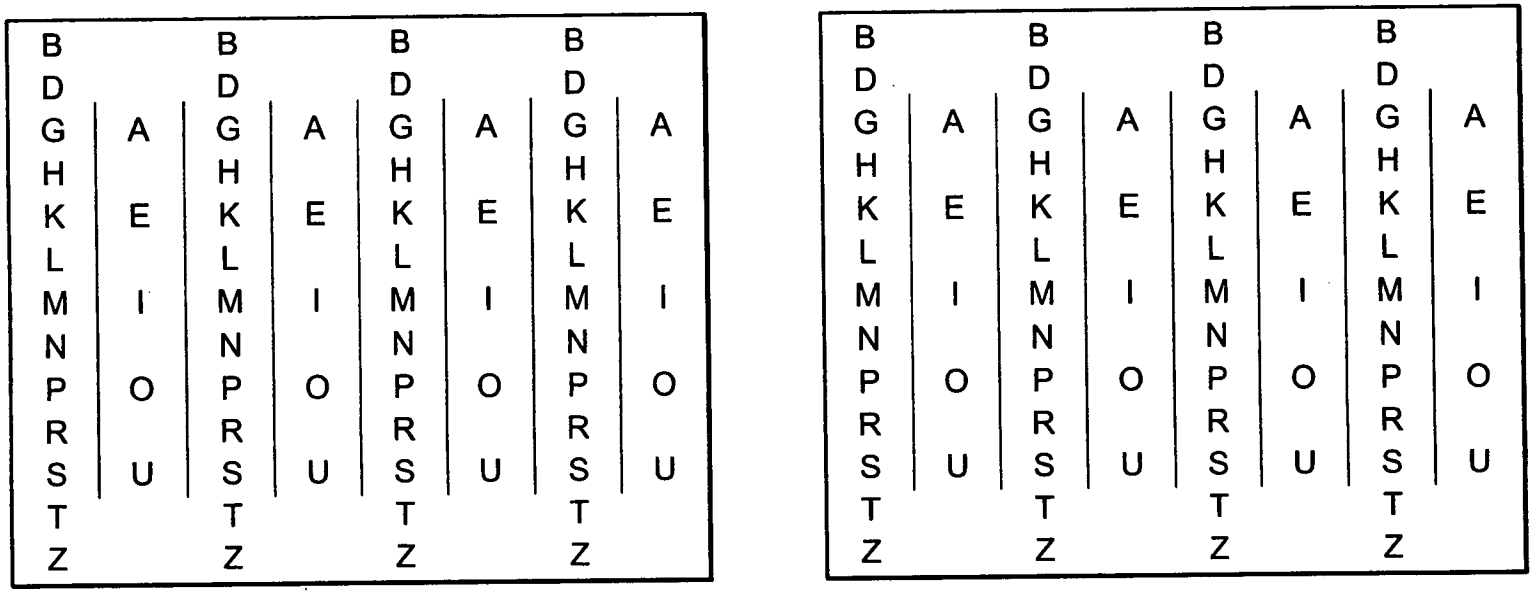


FIG. 12

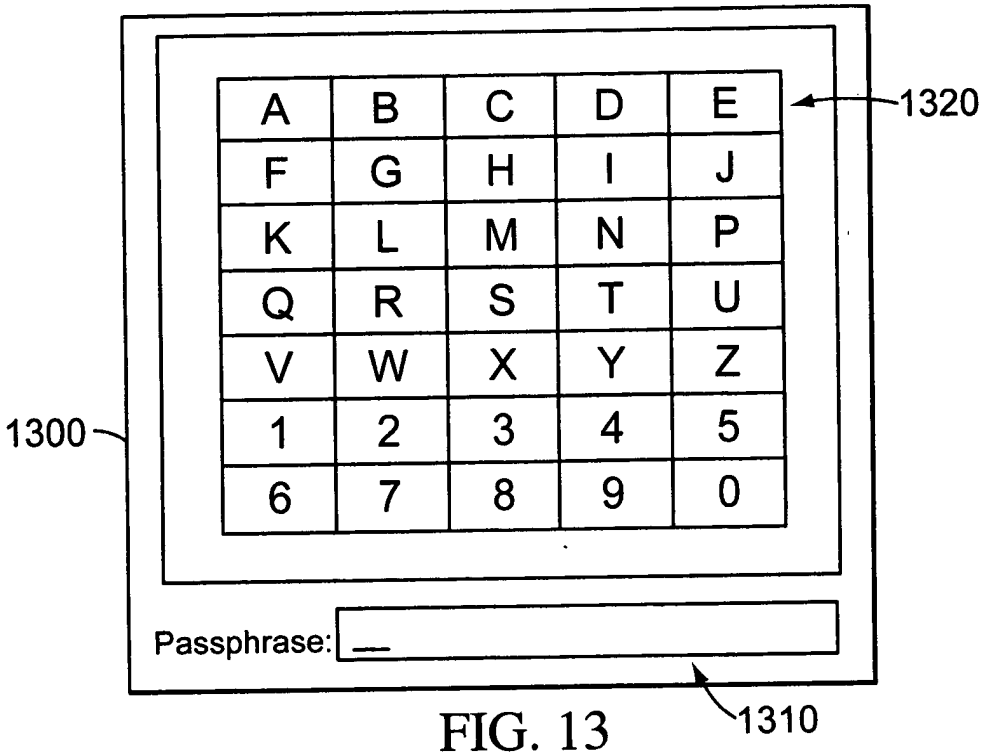

A B C D E
F G H I J
K L M N P
Q R S T U
V W X Y Z
1 2 3 4 5
6 7 8 9 0
1320
1300
Passphrase:
1310

FIG. 13

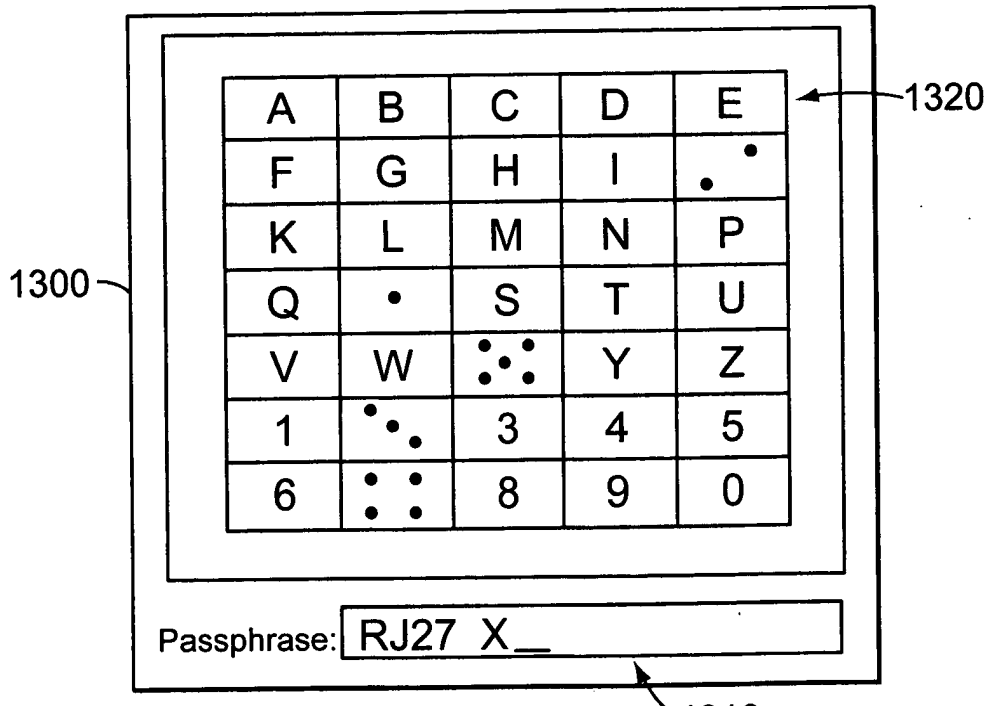

A B C D E
F G H I
K L M N P
Q S T U
V W Y Z
1 3 4 5
6 8 9 0
1320
1300
Passphrase: RJ27 X
1310

FIG. 14

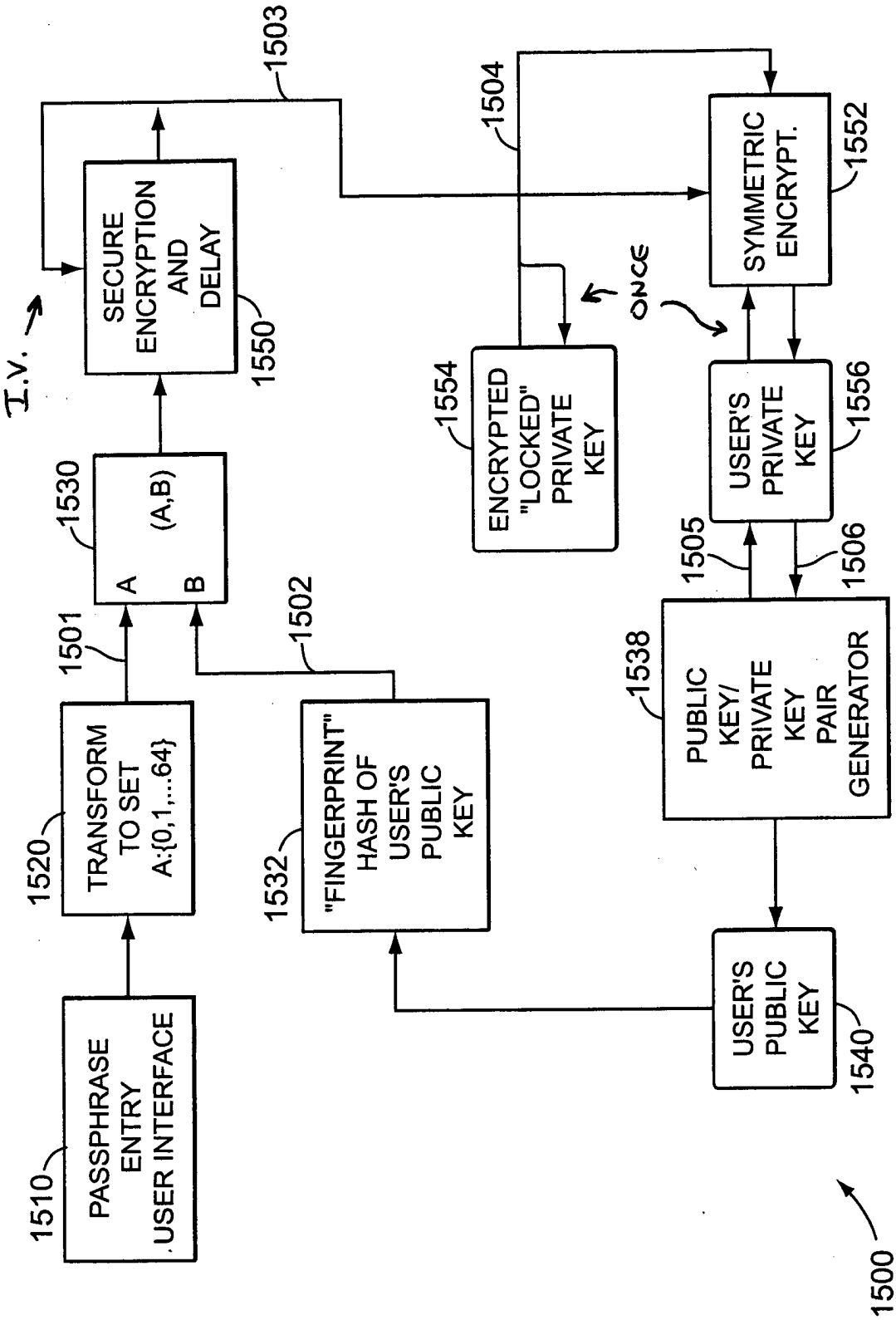

1500
1503
1504
1552
SYMMETRIC ENCRYPT.
SECURE ENCRYPTION AND DELAY
1550
I.V.
ONCE
1554
ENCRYPTED "LOCKED" PRIVATE KEY
1556
USER'S PRIVATE KEY
1530
(A,B)
A
B
1505
1506
1501
1502
1538
PUBLIC KEY/ PRIVATE KEY PAIR GENERATOR
1520
TRANSFORM TO SET A:{0,1,...64}
1532
"FINGERPRINT" HASH OF USER'S PUBLIC KEY
1540
USER'S PUBLIC KEY
1510
PASSPHRASE ENTRY USER INTERFACE

FIG. 15

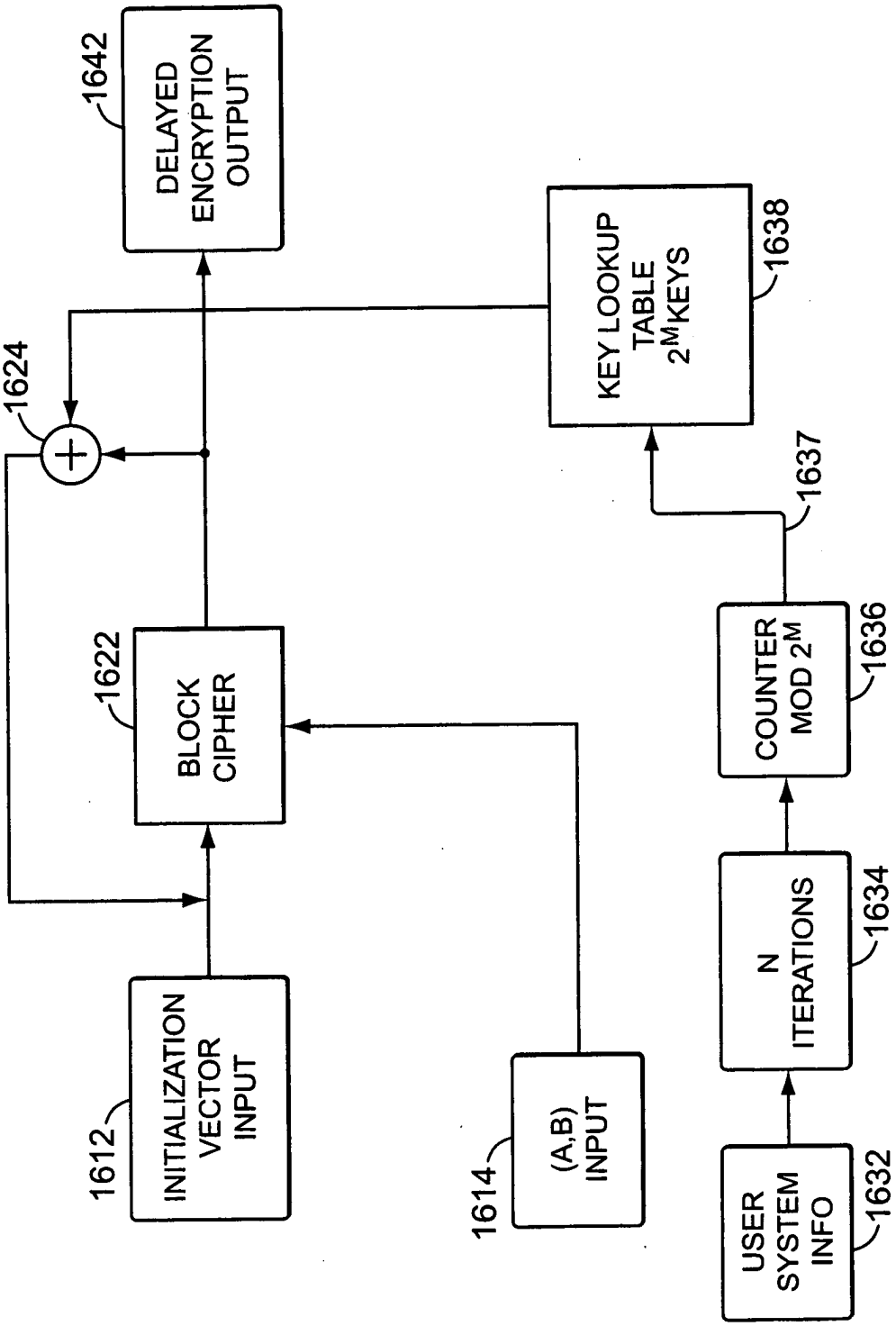

1642
DELAYED ENCRYPTION OUTPUT
1638
KEY LOOKUP TABLE 2^MKEYS
1624
1637
1622
BLOCK CIPHER
1636
COUNTER MOD 2^M
1634
N ITERATIONS
1612
INITIALIZATION VECTOR INPUT
1614
(A,B) INPUT
1632
USER SYSTEM INFO

FIG. 16

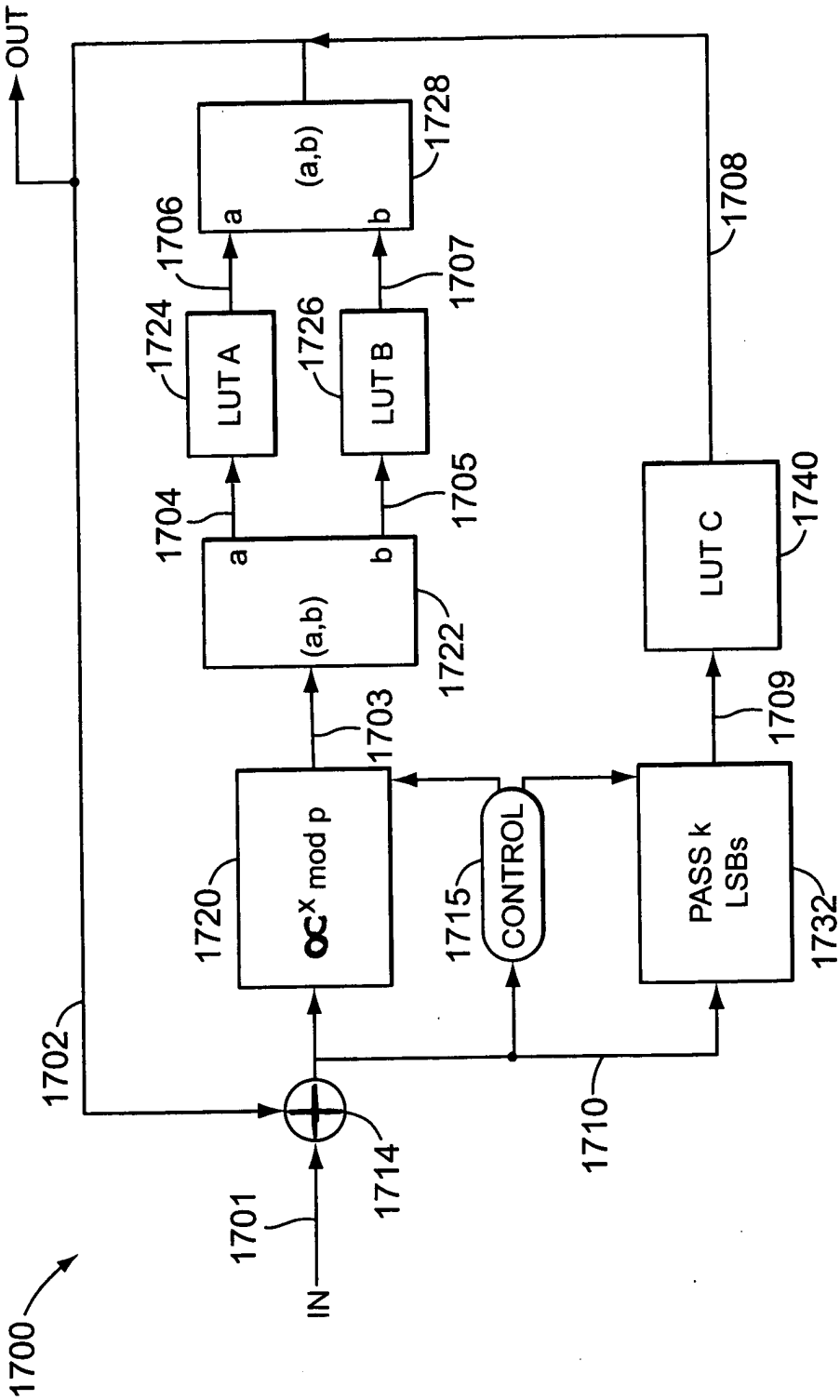

OUT
1728
(a,b)
a
b
1706
1707
1724
LUT A
1726
LUT B
1704
1705
(a,b)
a
b
1722
1703
1708
LUT C
1740
1709
1720
α^x mod p
1715
CONTROL
PASS k LSBs
1732
1702
1710
1714
1701
IN
1700

FIG. 17

FIG. 18

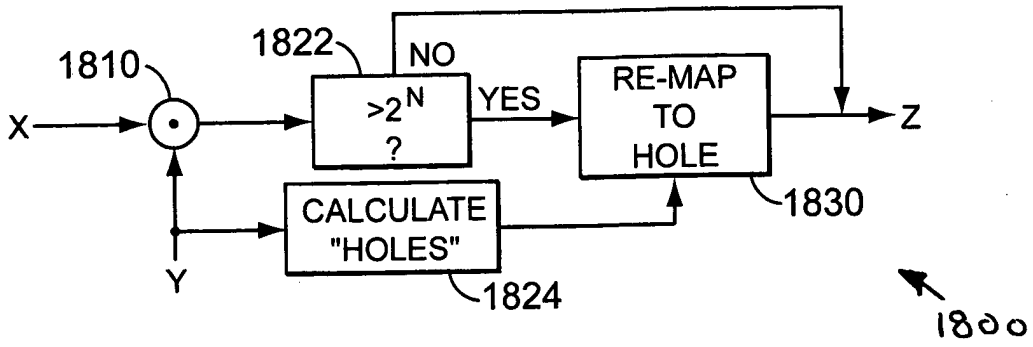


FIG. 19

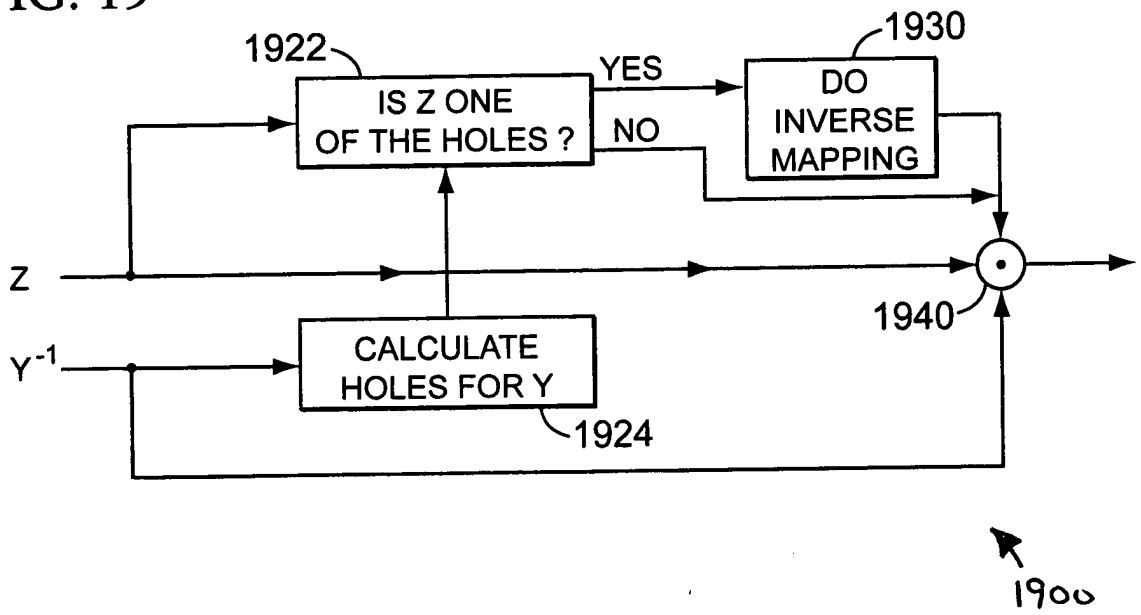


FIG. 20

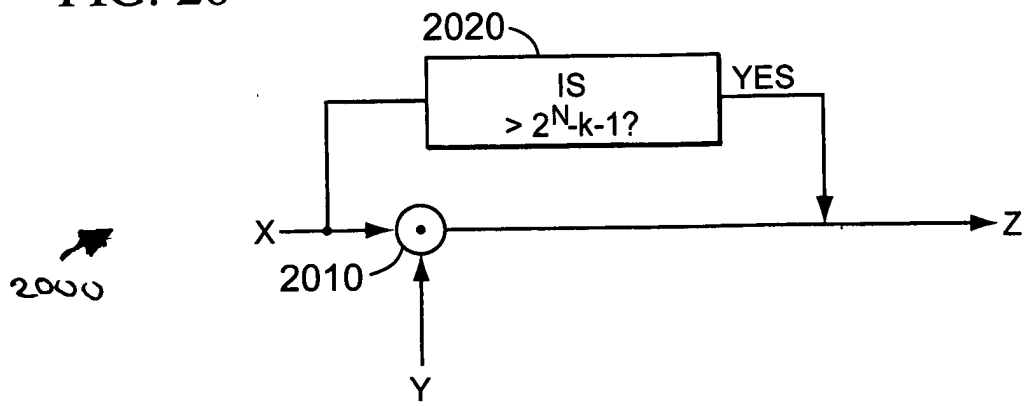
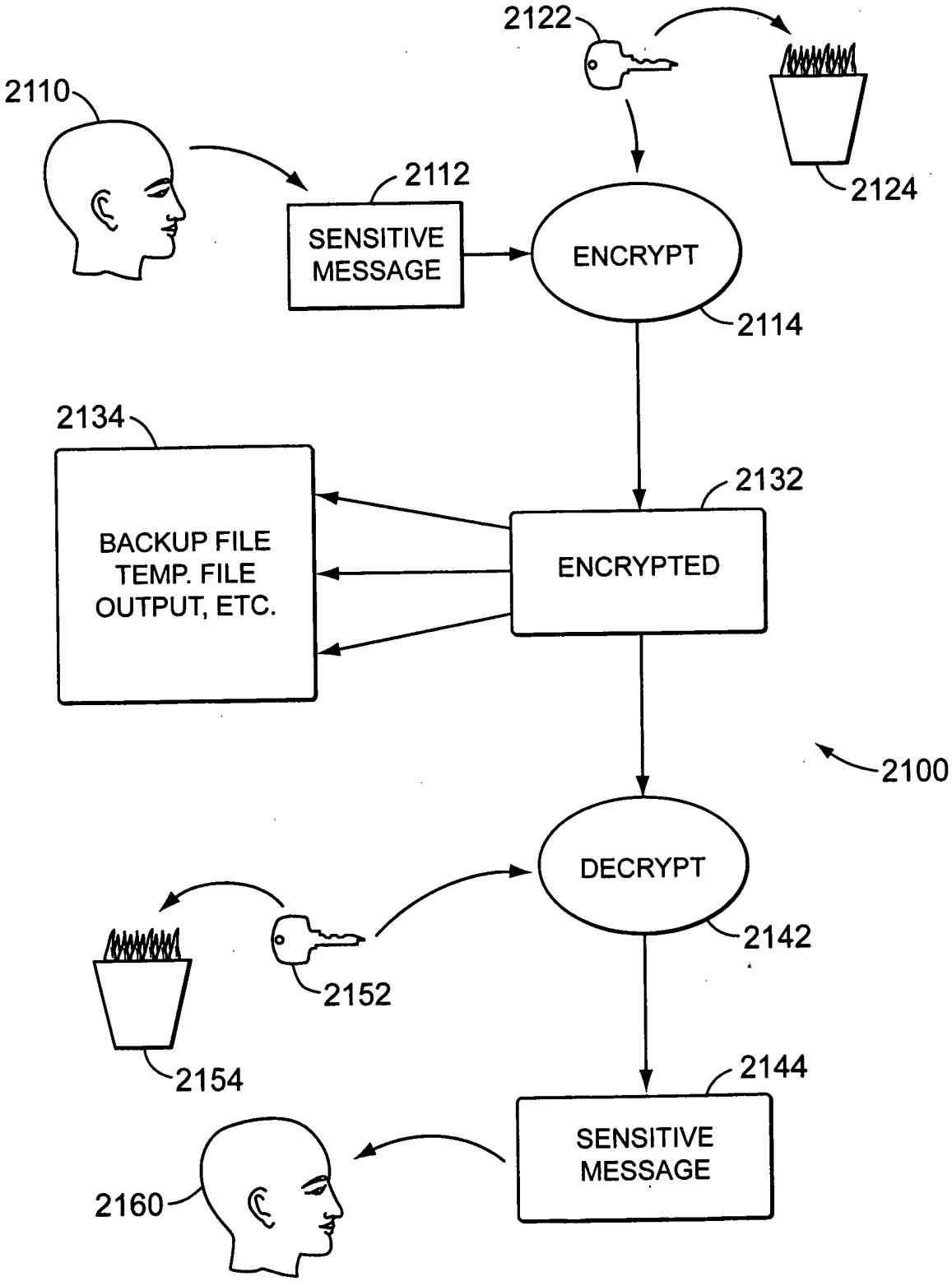


FIG. 21


2122
2110
2112
SENSITIVE MESSAGE
ENCRYPT
2124
2114
2134
BACKUP FILE
TEMP. FILE
OUTPUT, ETC.
2132
ENCRYPTED
2100
DECRYPT
2142
2152
2154
2144
SENSITIVE MESSAGE
2160